Alerta de seguridad informática	2CMV23-00435-01
Clase de alerta	Fraude
Tipo de incidente	Phishing-Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	16 de noviembre de 2023
Última revisión	16 de noviembre de 2023

PARA EL CORRECTO USO Y DIVULGACIÓN DE ESTE DOCUMENTO LEER ACÁ

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una nueva campaña de phishing con malware, distribuido en emails fraudulentos que lo llevan adjunto, argumentando falsamente que se trata de un veredicto judicial.

Este troyano bancario, llamado Grandoreiro, está dirigido a los países de Latinoamérica y es usado como puerta trasera para permitir al atacante acceder a los dispositivos de la víctima y así robar su información personal y bancaria en las sesiones de banca online que abra.

Grandoreiro requiere de la realización manual de una prueba de desafío-respuesta de tipo Captcha para ser ejecutado.

Indicadores de Compromiso Asociados

Archivos que se encuentran en la amenaza

SHA256

Indicador	Relación
429b7d4e94a270bbc55aad6c59e797d0604d4407d615a72b996f33ed9a837d26	RELACFFnaugHRBOqazxpqym.zip
6d34b216f9c95549b9e9be006e8bf15815ab437cd444ee7d2a0bafb165589a7b	CCFMANUSCReehmRCTZPPPQNUXT.exe
f2d850025dd7b65c44d979ec74a3f5a77e1c15b4070812be5656887cee95dc59	_____ _____ _____067 845966943.xml

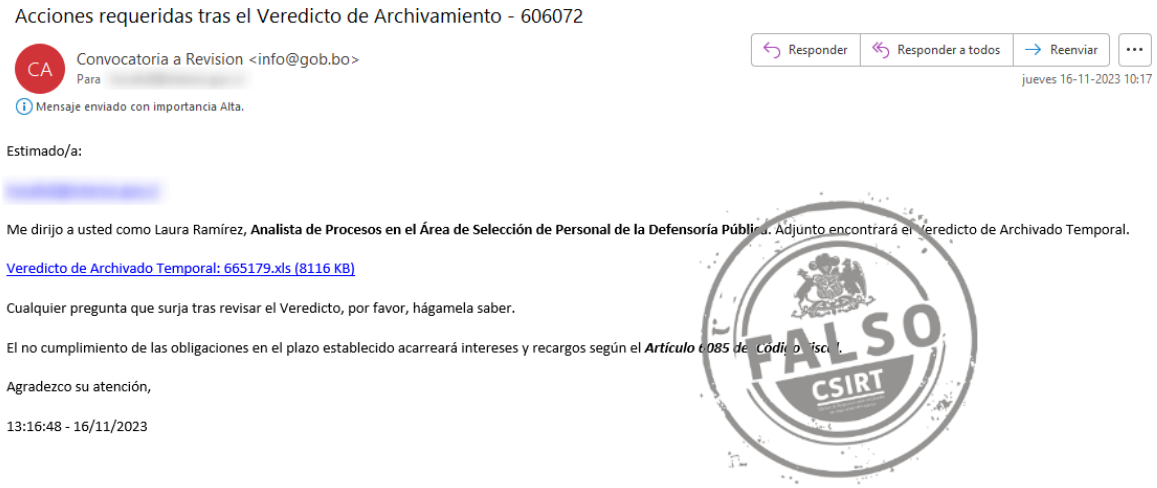
URL-Dominio

Dominio	Relación
https://visualizacionrnavegadorseguro.koreacentral.cloudapp[.]azure.com/visualizacion/	Descarga del Fichero
https://www.dropbox[.]com/scl/fi/aelie5ljeqzmp3rzsm89k/RELACFFuobrSXHCmtjptkzg.zip?rlkey=sn2od5814mebqr0w797z5vfta&dl=1	Directorio del Malware
http://54.232.33[.]91:40887/VsQHNzxx.xml	Archivo ZIP
http://ip-api[.]com/json	Whois
208.95.112[.]1	IP
54.232.33[.]91	IP

MITRE ATT&CK

Descripción	ID
Acceso Inicial (Mediante Phishing)	T1566.002
Descubrimiento (Descubrimiento de información del sistema)	T1082
Descubrimiento (Registro de consultas)	T1012
Persistencia (Carga lateral de DLL)	T1574.002

Imagen del Mensaje



Acciones requeridas tras el Veredicto de Archivamiento - 606072

CA Convocatoria a Revision <info@gob.bo>
Para [redacted]

Responder | Responder a todos | Reenviar | ...
jueves 16-11-2023 10:17

Mensaje enviado con importancia Alta.

Estimado/a:

[redacted]

Me dirijo a usted como Laura Ramírez, **Analista de Procesos en el Área de Selección de Personal de la Defensoría Pública**. Adjunto encontrará el Veredicto de Archivado Temporal.

Veredicto de Archivado Temporal: 665179.xls (8116 KB)

Cualquier pregunta que surja tras revisar el Veredicto, por favor, hágamela saber.

El no cumplimiento de las obligaciones en el plazo establecido acarreará intereses y recargos según el ***Artículo 6085 de Código Fiscal***.

Agradezco su atención,

13:16:48 - 16/11/2023

FALSO
CSIRT

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.11.17 15:32:45 -03'00'